UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,805	02/27/2004	Michael D. Smith	418268001US	5629

45979 7590 01/12/2012

PERKINS COIE LLP/MSFT
P. O. BOX 1247
SEATTLE, WA 98111-1247

EXAMINER	
GILKEY, CARRIE STRODER	
ART UNIT	PAPER NUMBER
3689	

NOTIFICATION DATE	DELIVERY MODE
01/12/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentprocurement@perkinscoie.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/789805
Filing Date: February 27, 2004
Appellant(s): SMITH, MICHAEL AND ABEL, MILLER

Maurice J. Pirio
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 09 December 2011 appealing from the Office action mailed 19 April 2011.

(1) Real Party in Interest

The Examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The Examiner is not aware of any related appeals, interferences, or judicial proceedings which will be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The following is a list of claims that are rejected and pending in the application:

Claims 1, 2, 5, 6, and 9-22 are pending and stand rejected. These claims are currently appealed. However, arguments were presented only for claims 1, 2, 5, 6, and 9.

(4) Status of Amendments After Final

Appellant states that an amendment is filed with their Appeal Brief in order to cancel claims 10-22. However, no such amendment was filed.

(5) Summary of Claimed Subject Matter

The Examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The Examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office Action from which the appeal is taken (as modified by any advisory actions) is being maintained by the Examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF RJECTION."

(7) Claims Appendix

Examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

20040153644	McCorkendale	02-2003
20030135509	Davis	01-2002
20010054026	Choate	02-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. **Claims 1, 5-6, 10-11, 13-15, and 17-22 are rejected under 35 U.S.C. 102(e) as being anticipated by McCorkendale et al. (US 20040153644).**

Referring to claim 1:

McCorkendale teaches

when installing an application (paragraph 56; "controls the installation and/or execution"),

establishing a limit on services of a service provider that the application is authorized to use based on published requirements of the application, the service provider being a computer system that is remote to the consumer system (paragraphs 36 & 51 & Fig. 1; "allows the software developer to securely transmit an application program or other piece of software to the certifying authority as part of a request to certify the software. Moreover, the module allows the software developer to receive a certified copy of the software back from the certifying authority" where "certifying authority" is interpreted as the service provider and the request to certify the software is interpreted as the "service" and "the frequency monitoring module tracks software execution frequencies over sliding time windows. For example, the module can track the number of execution requests for a particular piece of software in any given hour. If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious…the thresholds can be set based on trust level information included with the software" where the trust level information included with the software is interpreted as published requirements" and where the "certifying authority" in Fig. 1 is interpreted as the service provider and the "client device" is interpreted as the consumer computer);

asking the service provider if the application is authorized to use the service provider wherein the service provider determines that the application is not authorized based on notifications received from other consumer systems indicating that the application is misbehaving (paragraphs 49-50; "This module 522 is adapted to declare that software is potentially malicious upon the occurrence of an abnormally high frequency of requests from different client devices");

determining by the processor whether the application is authorized to request services of the service provider based on a response to the asking of the service provider if the application is authorized to use the service provider (paragraphs 49-50; "the malicious software detection module updates the software's status in the database module to 'deny'" and "is adapted to declare that software is potentially malicious upon the occurrence of an abnormally high frequency of requests from different client devices");

when it is determined that the application is authorized to request services of the service provider, installing the application (paragraphs 57-58; "allows the installation routine to install only approved software" and "this description uses the term 'execute' to mean 'execute and/or install'"); and

when it is determined that the application is not authorized to request services of the service provider, not installing the application (paragraphs 57-58; "allows the installation routine to install only approved software" and "this description uses the term 'execute' to mean 'execute and/or install'").

under control of a runtime environment after the application has been installed (paragraph 56; "controls the installation and/or execution"),

providing the application executing on the consumer system with access to an indication of the established limit so that the application can know and abide by the established limit (paragraph 58; where stopping the installation and/or execution of certain software is interpreted as an indication of the established limit and where "so that the application can know and abide by the established limit" is not a positive claim limitation and therefore, receives little patentable weight);

when the application executing on the consumer system requests a service of the service provider (paragraph 51 and 58; "the module can track the number of execution requests" where the service being provided is the granting or denial of permission for the software to execute and "Therefore, the present invention includes client devices 122 that perform the

gatekeeping function *during* (or prior to) installation of software and client devices that perform the gatekeeping function *during* (or prior to) execution of software." [emphasis added]),

determining by the processor whether the request would exceed the established limit that is based on published requirements of the application (paragraph 51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious");

when it is determined that the request would not exceed the established limit, requesting the service provider to provide the service (paragraphs 46-51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious" and "If the heuristics indicate that software is malicious, the malicious software detection module updates the software's status in the database module to 'deny'" and "the default status is 'allow' because the software is certified by the certifying authority and presumably safe"); and

when it is determined that the request would exceed the established limit (paragraph 51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious"),

notifying the service provider that the application is misbehaving (paragraphs 49 & 51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious" and "If the heuristics indicate that software is malicious, the malicious software detection module updates the software's status in the database module to 'deny'" and where updating the software's status in the database module is interpreted as notifying the service provider); and

prohibiting execution of the application on the consumer system (paragraphs 46-51; "If a client device requests to execute software marked as 'deny' in the database module, the detection module will report this status back to the client device, thereby preventing the software from being executed").

Referring to claim 10:

McCorkendale teaches

providing an indication of misbehavior for the application when the application requests services of the service provider, the service provider being a computer system that is remote to the consumer system (paragraphs 36 & 49-51 & Fig. 1; "If the heuristics indicate that software is malicious, the malicious software detection module updates the software's status in the database module to 'deny'" and "the frequency monitoring module

tracks software execution frequencies over sliding time windows. For example, the module can track the number of execution requests for a particular piece of software in any given hour. If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious…the thresholds can be set based on trust level information included with the software" and where the "certifying authority" in Fig. 1 is interpreted as the service provider and the "client device" is interpreted as the consumer computer);

executing by the consumer system the application (paragraph 58; "Therefore, the present invention includes client devices 122 that perform the gatekeeping function during (or prior to) installation of software and client devices that perform the gatekeeping function *during* (or prior to) *execution* of software." where *during execution* requires execution of the application by the consumer system) and

under control of a runtime environment executing on the consumer system (paragraph 56; "A gatekeeper module 612 in the client device 122 controls the installation and/or execution…"),

when the executing application requests a service of the service provider (paragraphs 9 and 51; "At some point, one or more of the client devices (122) attempts (714) to execute (as used herein, "execute" also includes "install") the software. As

part of this process, the client device (122) determines (716) whether the software is potentially malicious" and "the module can track the number of execution requests" where the service being provided is the granting or denial of permission for the software to execute),

determining by the processor whether the application is behaving in accordance with the indication of the misbehavior (paragraph 51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious");

when it is determined that the application is not behaving in accordance with the indication of misbehavior, requesting by the runtime environment, the service provider to provide the service (paragraphs 69; "If the client device 122 cannot determine whether the software is potentially malicious, i.e., its status is "unknown," the client device 122 typically blocks execution of the software and optionally sends 724 a copy of the software to the analysis authority 120 for evaluation."); and

when it is determined that the application is behaving in accordance with the indication of misbehavior (paragraph 51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious"),

notifying the service provider that the application is misbehaving so that the service provider can determine whether the application is misbehaving and revoke authorization of the application to use the service provider when executing on the consumer system or when executing on other consumer systems (paragraphs 49 & 51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious" and "If the heuristics indicate that software is malicious, the malicious software detection module updates the software's status in the database module to 'deny'" and where updating the software's status in the database module is interpreted as notifying the service provider); and

prohibiting continued execution of the application (paragraphs 46-51; "If a client device requests to execute software marked as 'deny' in the database module, the detection module will report this status back to the client device, thereby preventing the software from being executed").

Referring to claims 5 and 14:

McCorkendale teaches wherein the service provider aggregates notifications provided by different consumer systems to determine whether the application should be authorized to request services of the service provider (paragraph 50; "declare

that software is potentially malicious upon the occurrence of an abnormally high frequency of requests from different client devices to execute the same software within a relatively short time period").

Referring to claims 6 and 15:

McCorkendale teaches the service provider aggregates notifications provided by the consumer system to determine whether the consumer system should not be authorized to request services of the service provider (paragraph 50; "that detects potentially malicious software based on the frequency of software execution requests received from the client devices").

Referring to claim 11:

McCorkendale teaches wherein the indication of misbehavior is exceeding a number of requests for services of the service provider (paragraph 51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious").

Referring to claim 13:

McCorkendale teaches before installing the application determining whether the application is authorized to request

services of the service provider (paragraph 56; "software cannot be installed and/or executed without permission from it").

Referring to claim 17:

McCorkendale teaches

when service consumers determine that the application is misbehaving, receiving by the service provider notifications of the misbehavior from the service consumers, wherein the application misbehaves when the application requests certain services of the service provider, each service consumer being a consumer computer that is different from the computer system of the service provider (paragraphs 58-59; "Therefore, the present invention includes client devices 122 that perform the gatekeeping function during (or prior to) installation of software and client devices that perform the gatekeeping function during (or prior to) execution of software. In a similar manner, the frequency monitoring module 522 in the execution authority 118 can utilize installation and/or execution frequency statistics to detect malicious software.");

determining by the processor whether a condition of misbehavior is satisfied based on the received notifications from different consumers indicating that the application is misbehaving when executed by the different consumers (paragraphs

49-50; "the malicious software detection module updates the software's status in the database module to 'deny'" and "is adapted to declare that software is potentially malicious upon the occurrence of an abnormally high frequency of requests from different client devices"); and

when a service request is received to provide services to the application and it is determined that the condition of misbehavior is satisfied, refusing to provide the requested service (paragraphs 46-51; "If the number of executions exceeds a predetermined threshold, the module determines that the software is malicious" and "If a client device requests to execute software marked as 'deny' in the database module, the detection module will report this status back to the client device, thereby preventing the software from being executed").

Referring to claim 18:

McCorkendale teaches wherein the condition of misbehavior is when multiple service consumers provide notifications that the application has attempted to exceed an established limit of requests for services from the service provider (paragraph 50; "adapted to declare that software is potentially malicious upon the occurrence of an abnormally high frequency of requests from different client devices").

Referring to claim 19:

McCorkendale teaches receiving from another service provider a notification that the application is misbehaving wherein the condition of misbehavior is satisfied based on the notification received from another service provider (paragraph 32; "the execution authority notifies the analysis authority when the execution authority detects a possible software worm" and where the execution and analysis authorities are interpreted as service providers).

Referring to claim 20:

McCorkendale teaches notifying service consumers that the application is not authorized to request services of the service provider (paragraph 52; "this module sends 'malicious software' alerts to the client devices").

Referring to claim 21:

McCorkendale teaches wherein a service consumer requests the service provider to indicate whether the application is authorized (paragraph 36; "this module allows the software developer to securely transmit an application program or other piece of software to the certifying authority as part of a request to certify the software" and where the software

developer is interpreted as a service consumer and the certifying authority is interpreted as the service provider).

Referring to claims 22:

McCorkendale teaches wherein the condition of misbehavior is based on an aggregation of the service consumer notifications (paragraph 50; "declare that software is potentially malicious upon the occurrence of an abnormally high frequency of requests from different client devices to execute the same software within a relatively short time period").

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

1. **Claims 2 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over McCorkendale et al. (US 20040153644) as applied to claims 1 and 10 above, in view of Davis et al. (US 20030135509).**

Referring to claims 2 and 12:

McCorkendale does not disclose wherein the prohibiting includes uninstalling the application. However, Davis discloses wherein the prohibiting includes uninstalling the application (paragraph 64).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the teaching of McCorkendale by uninstalling the application as taught by Davis because this would provide a way to completely remove an application that was misbehaving, thereby preventing a possible virus.

2. **Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over McCorkendale et al. (US 20040153644) as applied to claim 1, above, in view of Choate (US 20010054026).**

Referring to claim 9:

McCorkendale does not teach wherein multiple service providers can provide equivalent services and the application can requests services one of those service providers as designated by the consumer system. However, Choate teaches wherein multiple service providers can provide equivalent services and the application can requests services one of those service providers as designated by the consumer system (paragraph 26).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the teaching of McCorkendale as taught by Choate because this would provide the ability to continue to provide services to customers while the system is fixed.

3. **Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over McCorkendale et al. (US 20040153644) as applied to claim 10, above, in view of Choate (US 20010054026).**

Referring to claim 16:

Liang does not teach wherein the limit is established by a user of a consumer system. However, Choate teaches wherein the limit is established by a user of a consumer system (paragraph 31).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the teaching of McCorkendale by allowing the user to establish a limit as taught by Choate because the user is the one who is actually using the services and is in the best position to determine what is abnormal, which would provide a more accurate assessment of whether the system is misbehaving.

(10) Response to Argument

The applicant makes introductory remarks under part "C. Discussion of the Issues" (page 8 of Appeal Brief), stating that McCorkendale's invention and appellant's invention function in fundamentally different ways. Applicant admits that McCorkendale prevents execution of software and states that applicant's invention "…prevents installation of an application…", but that McCorkendale does not prevent installation of an application. Examiner respectfully disagrees. McCorkendale states, in [0058] that the "descriptions uses the term 'execute' to mean 'execute and/or install.'"

1. The Examiner does not take inconsistent positions when rejecting the claims.

Applicant argues that Examiner is using different features of McCorkendale to correspond to the claimed "service" and as such, is taking inconsistent positions. Examiner respectfully disagrees. The first service being referred to by applicant is in the second limitation "establishing a limit on services of a service provider…" and the second service being referred to by applicant is state in the ninth limitation "when the application

executing on the consumer system requests a service of the service provider." This ninth limitation states that the application is requesting a service, not the service. These services are two different services in the claim as written, not the same service. Therefore, Examiner is not taking inconsistent positions. However, even if the service being referred to was the same one, "service" is a broad term and is not limited to one particular service; it could include several different services being offered.

Applicant also argues that it is inconsistent for the Examiner to use both the "certifying authority" and "execution authority" as mentioned in McCorkendale as the "service provider" in the claims. Examiner respectfully disagrees. First, as is mentioned above, the claims refer to "a service" in the ninth limitation, which is a different service from the service mentioned in the second limitation. As such, the service providers may be different. Second, the term "service provider" is broad enough to encompass both the certifying and execution authorities.

2. The McCorkendale features that correspond to the claimed elements are arranged as claimed.

Applicant argues that McCorkendale does not "…suggest that any limit is placed on requests to certify of a certifying authority." Examiner respectfully disagrees. McCorkendale states, in [0051], "…the module can track the number of execution requests…" This is a limit on the number of services allowed before the software is declared malicious, since a certifying request is part of an execution request and is the service being provided.

Applicant also argues that the prior art does not disclose "when the application executing on the consumer system requests a service of the service provider." Examiner respectfully disagrees. The gatekeeper module 612 is requesting permission for the software to install or execute on behalf of the software. This gatekeeper module is invoked by the software's attempt to install or execute [0057]. Therefore, the application is requesting a service, albeit through the gatekeeper module.

3. McCorkendale discloses "determining by the processor whether the request would exceed the established limit that is based on published requirements of the application."

Applicant argues that "the claims recite that the consumer system determines 'whether the request would exceed the established limit'…and if so, it notifies 'the service provider that the application is misbehaving'" and that McCorkendale does not disclose this feature of the claim. Examiner respectfully disagrees. First it is necessary to determine exactly what the claim recites, as applicant argues that the claim language includes more than is actually included in the claim. The claim states only that "the processor" determines "whether the request would exceed the established limit" NOT that the consumer system makes the determination, nor that the consumer system performs the notification step. It is not recited who or what performs the notification step. The processor which is recited as performing the determining step is recited in the preamble, which states, "A method in a consumer system with a processor and a memory..." This does not indicate that the processor is part of the consumer system, merely that it performs in concert with the consumer system. McCorkendale does provide a processor which performs the determining step (see [0051], which states that the frequency monitoring module 522, performs the determining step, and since a software module cannot execute without the use of a processor, the processor is performing the

determining); therefore, McCorkendale discloses this feature as claimed.

Further, even if the processor is part of a consumer system, and not merely performing in concert with the consumer system (as is understood from the preamble), the information from the frequency monitoring module 522 is transmitted to the consumer, or client device 122, through the gatekeeper module 612, which actually stops the software from installing or executing ([0056]-[0057]). Therefore, the client device is performing a determination that the request exceeds the established limit and should not be allowed to execute.

Only arguments pertaining to claims 1, 2, 5, 6, and 9 were presented for appeal. Therefore, the rejections for claims 10-22 stand.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the Examiner in the Related Appeals and Interferences section of this Examiner's Answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Carrie Stroder Gilkey

/CARRIE STRODER GILKEY/

Examiner, Art Unit 3689

Conferees:

Gerardo Araque

/Gerardo Araque Jr./
Primary Examiner, Art Unit 3689

/Dennis Ruhl/
Primary Examiner, Acting Supervisor, Art Unit 3689